Chapter 31 - Physical Security Planning

3101 Security Planning

A. The heads of operating units and senior managers responsible for Department of Commerce facilities shall ensure that security planning is an integral part of any function or project undertaken within the Department. Selecting, constructing, or modifying a facility without considering the security implications of employee safety and asset protection can result in costly modifications or retrofitting, considerable lost time, and liability for the Department.

B. All security standards will be met in new or altered facilities whether constructed or acquired by purchase or lease. Every attempt will be made to acquire sites or new facilities that facilitate meeting physical security standards. In the event that one or more security standards may not be possible for a specific building, requests for exceptions shall be requested by the departmental organization to the Director for Security.

C. Physical security programs shall be established and implemented within each operating unit based on the minimum standards set forth in the manual and other appropriate laws, regulations, and national codes for the protection of life and property to ensure the protection of departmental personnel and assets. The programs shall be administered and monitored to ensure their integrity. At a minimum a unit physical security program shall include the following elements.

1. A physical security survey for each facility occupied by departmental personnel;

2. Scheduled/unscheduled inspection of facilities to determine if the local security program meets required Federal and departmental standards or regulations;

3. A comprehensive and continuing security education and awareness effort to gain the interest and support of employees, contractors, consultants, and visitors;

4. An established process of emergency procedures to take immediate, positive, and orderly action to safeguard life and property during an emergency; and

5. An appropriate set of security procedures to respond to changing threat conditions.

D. The survey will evaluate the capability of the facility to protect departmental personnel, assets, and information. The interior and exterior portions of a facility should be videotaped for the record.

3102 Facility Protection

A. The senior facility manager shall determine the level of protection required for each facility under his or her control based on the results of a comprehensive security survey of the facility. The survey will identify the jurisdictions involved and required responses. Formal agreements with local protective service companies or law enforcement agencies may be required to ensure proper responses. At a minimum a unit physical security program shall consider the following criteria.

1. Perimeter protection is the first line of defense in providing physical security for personnel, property, and information at a facility.

2. Interior controls as the second line of defense are perhaps the most important. The extent of interior controls will be determined by considering the monetary value and criticality of the items and areas to be protected, the vulnerability of the facility, and the cost of the controls necessary to reduce that vulnerability.

3. Cost of the security controls normally should not exceed the monetary value of the item or area to be protected unless necessitated by criticality or national security.

B. Departmental facilities that handle, store, or process Top Secret classified information are required to employ guard services or other appropriate response forces to protect that information. Guard services may be provided at other departmental facilities after coordination between the facility manager and the servicing security officer. A security survey of the facility will determine the type and size of guard service. Any new security guard requirement shall be supported by a security survey.

3103 Planning Facility Protection

A. The objective of planning facility protection is to ensure both the integrity of unit operations and the security of personnel, property, and information. Security requirements must be integrated into the site selection and construction or renovation before moving into a departmental facility.

B. The modification of a facility or addition of security measures after occupying a facility can be costly and impractical; therefore, the facility manager and the security officer need to define the security measures necessary to support the facility's mission and work prior to any construction or renovation. Coordination shall begin with the designers and architects and continue through the contracting process and construction and installation.

C. Many Department of Commerce offices occupy space in commercial buildings where GSA executes the lease for the Department. In leased office space with multiple tenants, access may not be controlled to the same extent as in a facility where the Department is the sole tenant. When the Department is the sole tenant, the security contact has more flexibility to plan and implement access controls. In most multi-agency tenant buildings, departmental tenants must rely on GSA to provide protection for the building. When GSA provides security, departmental security contacts and administrative officials must establish a working relationship with the appropriate GSA officials and maintain an active role in the security decisions and processes that affect the facility.

3104 Design Factors

A. Introduction. Security systems and procedures shall be considered from the design stage to the completion of the project. Conduit runs, alarm wiring, utility access, reinforcing devices, and other necessary construction requirements should be included in the original design and construction plans. In addition to the factors listed below, see other chapters in this manual for further guidance concerning design and construction of physical security systems.

B. Facility and Building Location.

1. **Access Requirements.** The planner must review the mission of the facility and determine the level of public access required, the time it will take for personnel to respond to incidents during duty and non-duty hours, and the workflow and processes so security can be integrated into the facility.

2. **Geographical Factors.** The planner must consider approach routes, traffic patterns, and nearby transportation. If possible, facilities should not be located near high crime, high traffic, or industrial areas.

3. **Building Configuration.** At a facility site, the number of separate buildings should be kept to a minimum and grouped close together. Close-in access for vehicles shall be discouraged. Barriers or passageways should be constructed to permit employees and property to pass safely between buildings.

C. Configuration of Space.

1. **Entrances.** Facility or office entrances should be kept to the absolute minimum, yet comply with fire safety codes. Although employee access, parking, and deliveries are to be accommodated, security-maintained entrances shall be engineered with provisions for guard posts and access control systems. One entrance with multiple interior routes is preferable to

several outside entrances. Plans shall include space for reception desks, barriers, and other controls.

2. **Access Controls.** Locking devices shall be used on all perimeter and interior doors. These devices can be either key or electronically operated. Cleaning, maintenance, and protective staff need access to do their jobs. Keys, Personal Identification Numbers (PIN), and time zones shall be defined to support these functions.

3. **Location of Offices and Facilities.** Offices or other facilities should be adjacently located and on the same or successive floors. Facility managers should try to avoid leasing space that has non-departmental leased space between departmental leased space. Sensitive operations such as credit unions, imprest funds, or those involved in handling classified or sensitive information should be located on upper floors and away from entrances. Related activities, such as shipping and receiving should be located in adjacent or nearby locations (see paragraph 3806, Shipping/Receiving and Storage Areas). To control access to the spaces, facility managers shall install locks on entrances/exits and corridor doors. Perimeter doors and interior rooms will be locked when unattended. Key issuance and control programs must be established.

4. **Guard Forces.** Access controlled by a guard force requires written procedures to define who can enter the facility. When a guard service is not used or available, facility managers shall establish a liaison with local law enforcement officials and advise them of the security hours and who to contact in an emergency. If necessary, facility managers shall arrange for the protection of employee parking areas.

5. **Property Control.** Facility managers shall establish procedures to provide for the control and removal of property, equipment, and official records. Signature exemplars of property pass holders must be maintained on file and utilized by the guard force to control improper removal of property, equipment, and official records.

D. Safety and Fire Protection. Safety and fire protection requirements must be incorporated into any construction plans. Operating units must follow accepted fire prevention practices in operating and managing buildings. Federally owned buildings are generally exempt from state and local code requirements in fire protection. In accordance with Title 40 of the U.S. Code § 619, however, each building constructed or altered by a Federal agency must be constructed or altered, to the maximum extent feasible, in compliance with one of the nationally recognized model building codes and with other nationally recognized codes. Operating units in the Department of Commerce must use the National Fire Protection Association (NFPA) codes and standards as a guide for their building operations. Managers shall contact GSA and/or appropriate officials regarding GSA requirements, NFPA codes, and possible local code requirements and construction standards when constructing or altering Federal facilities.

E. Utilities. Utility systems shall be protected against unauthorized access. The protection of telephone, electrical, heating and cooling systems, water supplies, boilers and generators, and valves, regulators, and controls must be planned.

F. Special Activities. Special emphasis shall be placed on security systems and safeguards when constructing or modifying special or sensitive activities such as mail rooms, equipment storage or shipping and receiving areas, classified work areas, computer rooms, child care centers, and special use areas such as warehouses or hazardous materials storage areas. Additional information is contained in Chapter 38, Security for Special Functions.

G. Contingency Plans. A contingency plan must be developed for each Department of Commerce facility to protect personnel and property in the event of emergencies such as fire, bomb threats, civil disturbances, and natural disasters. See Appendix R, Homeland Security Phased Security Alert Levels and Appendix S, Bomb Threat Procedures.

3105 Surveys and Inspections

A. Introduction. A physical security survey is an in-depth analysis used to determine security measures needed to protect departmental personnel, property, and information. An inspection is a check or test against a set of standards or regulations to verify if a security program or facility meets those standards or regulations. Inspections evaluate implementation of regulations, the education of employees, security administration, and existing internal management controls. The facility manager shall use surveys and inspections to carry out oversight responsibilities.

B. Physical Security Surveys.

1. **Purpose.** The facility manager, in conjunction with the servicing security officer, will conduct a survey of each facility under his/her jurisdiction to determine the type and extent of security controls necessary for each facility or area. Each physical security survey will include a security evaluation (risk assessment) that addresses the criticality of operations, the vulnerability of the facility or area, the probability of loss or damage to the facility or property and danger to personnel, and recommended countermeasures presented on a cost-benefit basis.

2. **Checklists.** When an on-site visit by the servicing security officer is not possible, the facility manager will conduct a self-administered checklist survey and forward a copy of the checklist to the servicing security officer. A checklist is a detailed questionnaire, as illustrated in Appendices L, N, O, or P that addresses facility security issues. The checklists are furnished as general guides since not all of the questions apply to all facilities. All "Yes" answers on a checklist are not necessarily a requirement for a secure facility or an indication of a totally

secure facility. The facility manager will have to make decisions concerning the applicability of each question to the particular facility or space being surveyed.

3. **Recommendations.** The servicing security officer shall assist the facility manager in developing a security plan to address recommendations resulting from the surveys, inspections, or self-administered checklists. All recommendations shall be coordinated with the Office of Security.

4. **Criticality, Vulnerability, and Probability.** A survey is not complete until the factors listed below have been given full consideration.

a. **Criticality.** Criticality defines the effect that work reduction or mission loss would have on a facility or operation. Work loss or reduction could have a negative impact on national security, departmental mission, or a facility's operations. Examples of adverse effects include the interruption of a vital function, disruption of operations, or the compromise of classified information. A higher classification level of information processed or stored in a facility will increase the *criticality* factor at that facility.

b. **Vulnerability.** Vulnerability describes the susceptibility of a facility or operation to damage, destruction, possible theft, or loss of property. Physical *vulnerability* factors include the size, configuration, construction, and location of the facility. Area *vulnerability* factors include population demographics, the local crime rate, the proximity of law enforcement, and emergency response services.

c. **Risk.** Risk evaluates the potential for damage or loss to a departmental operation, activity, facility, or mission. A risk assessment is conducted to determine the probability that an action, circumstance, or event could cause loss or damage to a departmental asset. Probability of risk is an ever-changing dynamic that depends on the intention and capability of an adversary to undertake actions detrimental to departmental interests.

5. **Types of Surveys.**

a. **Initial Survey.** The initial survey is conducted prior to constructing, leasing, acquiring, modifying, or occupying a facility or area. It identifies security measures or equipment necessary to maintain the level of security required to protect the facility dictated by the criticality and vulnerability of the facility.

b. **Compliance Survey.** After the initial survey, a compliance survey is conducted to ensure the completion of specified modifications. This survey shall be conducted before acceptance of the property or occupancy.

c. **Supplemental Survey.** A supplemental survey is conducted when significant changes in organization, mission, or facility structure occur. The survey is conducted at the discretion of either the facility manager or the servicing security officer.

d. **Special Survey.** The special survey is conducted to examine or resolve specific issues, such as the accreditation of a vault used to store Sensitive Compartmented Information (SCI) material or an assessment of damage resulting from an incident. Special surveys are initiated at the direction of the Director for Security.

6. **Conducting Surveys.** The servicing security officer shall conduct a survey with the assistance of the facility manager. The facility manager will provide a layout of the facility depicting interior areas in the facility, access points, parking lots, warehouses, and any adjacent areas belonging to the facility. The servicing security officer shall interview program management officials to determine the mission and nature of operations, classification or sensitivity level of information, and value of assets. He or she should visit the facility or area to obtain the information noted below.

a. The facility's address, number of buildings, tenant organizations, approximate population, and names of key management officials.

b. The security level of the building as determined by the Department of Justice Vulnerability Assessment of Federal Facilities.

c. Type of construction of buildings at the facility.

d. A description of features of the facility and conditions that produce vulnerabilities. The physical configuration of the office or facility storing classified information shall be documented.

e. A description of adjacent buildings that could provide access to the facility.

f. A description of the surrounding area, e.g., types of buildings, terrain, vegetation, roadways, pedestrian walkways, parking lots, etc., for at least one quarter of a mile in all directions. The area should be expanded if significant crime demographics are developed.

g. An analysis of criminal and fire incidents for the jurisdiction(s) in which the facility is located covering at least a one-year period. Crime/fire records should be obtained for the surrounding area of the facility and compared to the facility records.

h. The law enforcement agency, fire department, guard force company or agency, and other organizations responsible for emergency response along with its response time.

i. An assessment of the replacement and/or intrinsic value of assets, and sensitive or unique equipment. The highest classification level of information processed or stored in the facility and the number and types of weapons should be documented.

j. A description of access controls, alarms, guard services, and security containers.

k. Recommendations for improving security and pertinent implementing instructions.

7. **Survey Report.** The servicing security officer, in coordination with the facility manager, will ensure that the survey report is thorough and precise. The survey report shall be submitted to the facility or office manager for review prior to completion of the recommendations. A copy of the completed survey report shall be maintained by the servicing security officer and a copy forwarded to the Office of Security for review. The survey report should include:

a. The rationale for the survey;

b. A security evaluation;

c. A background or history, if applicable;

d. A paragraph describing the environment around the facility;

e. A detailed statement of findings and recommendations for making any necessary security improvements; and

f. The exhibits supporting the report such as floor plans, photographs, and specifications.

C. Physical Security Inspections.

1. **Purpose.** Inspections, announced or unannounced, are conducted to determine the extent of compliance with security regulations and procedures to ensure the protection of the Department's assets. The facility manager will periodically conduct self-administered inspections of facilities and programs under his/her jurisdiction as necessary to ensure compliance with the provisions of the manual. The Office of Security will provide oversight through a compliance review and assistance visit conducted by the servicing security officer or a compliance review team. The inspections will result in a written report with copies retained at the inspection site and with the servicing security officer and the Office of Security.

2. **Recommendations.** The servicing security officer and/or the compliance review team will assist the facility or office manager in resolving any discrepancies or implementing any recommendations.

3. **Types of Inspections.**

a. **Evaluative** or **Fact-Finding Inspection.** Promotes a positive tone, while taking a broad, general look at a facility or program. The inspector has the option to resolve the deficiency on the spot or recommend further corrective actions within a non-specified time frame. The evaluative inspection can assist management officials in planning or upgrading their security programs.

b. **Compliance Inspection.** Focuses on compliance with established standards or regulations and may be admonitory in tone.

c. **Penetration Inspection.** A deliberate attempt by security officials to breach security systems and procedures to test compliance with regulations and procedures and is usually conducted for counterintelligence purposes at facilities where highly classified and/or critical operations or materials are at risk from hostile intelligence operations. A penetration inspection must be approved, in advance, by the Director of Security.

d. **Self-Inspection.** Initiated by the facility manager or security contact to evaluate his or her own security program. The initiator determines the scope and purpose of the self-inspection. Checklists in the manual (Appendices L – Q) can be adapted for self-inspection surveys. Further guidance on self-inspections can be obtained from the servicing security officer, facility manager, or the Office of Security.

4. **Frequency of Inspections.** The frequency of inspections will be based on the criticality and vulnerability of a facility or the level of classification or value of information processed or stored at a facility. The following guidance provides the minimum frequency for inspections.

a. Facilities that process or store Sensitive Compartmented Information, Communications Security (COMSEC), or NATO information shall be inspected annually.

b. Facilities that process or store Top Secret information shall be inspected every two years.

c. Facilities that produce highly critical or sensitive information, or have been designated highly vulnerable to damage, alteration, or disruption, shall be inspected every three years.

d. All other Department of Commerce facilities shall be inspected every five years.

e. After-hours room checks shall be conducted randomly or as needed.

5. **Conducting Inspections.** The following guidance provides the minimum steps for conducting inspections.

a. The inspector shall determine the scope, type, and method of inspection. The inspection must be scheduled with the office or resident facility manager, and if appropriate, written notice shall be provided. The notice should provide the dates, purpose, proposed interview schedule, and a request for any additional information, as needed. The inspector should review past inspection reports and mission statements and prepare a list of questions or a checklist to structure the inspection.

b. Upon arrival at the site and prior to departure, the inspector shall meet with the security contact and the facility manager or his or her representative to discuss the inspection. A sufficient sampling of data shall be collected from interviews with on-site employees and contractors and from touring the facility. The inspector will review the facility's local security procedures. After the review, the inspector shall report all findings to include any discrepancies corrected on the spot.

c. After sufficient data is collected, the inspector should analyze all findings, compare them with applicable security regulations, list discrepancies and cite regulatory references, recommend corrective actions, and write the inspection report.

d. The inspection report shall be produced within 20 working days of completion of the inspection. It should be divided into sections consisting of a summary, introduction, scope and purpose, overview and methodology, findings and recommendations, and observations. The report should be distributed to the security contact and the manager of the facility inspected in a timely manner. The report will require a response to any recommendations not later than 60 working days from the date of report.